

SRE Day 2026: Helping Organisations Prepare for Disasters Using Cyber Continuity

Presenter: Charles Weir

Lancaster University

MANCHESTER 1824

Contributors:
Cecilia Loureiro-Koechlin
Louise Dennis, Lucy Hunt,
Ita Ryan

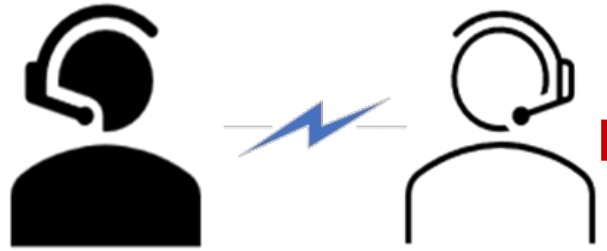
UCC
University College Cork, Ireland
Coláiste na hOllscoile Corcaigh

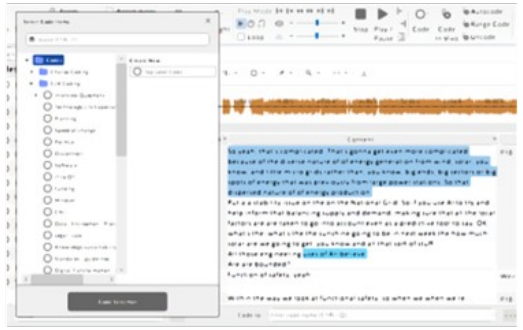


Why this matters… some prior research:

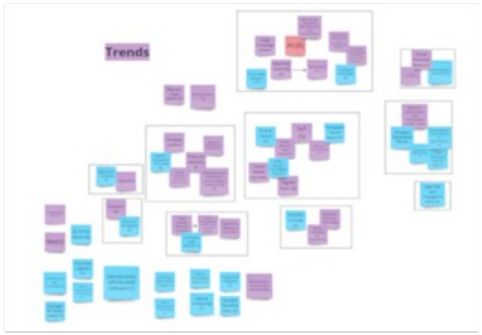
What effect may changes in software systems between now and 2040 have on major incidents related to UK Critical National Infrastructure (CNI)?

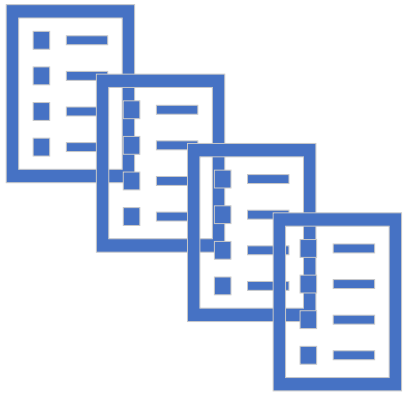












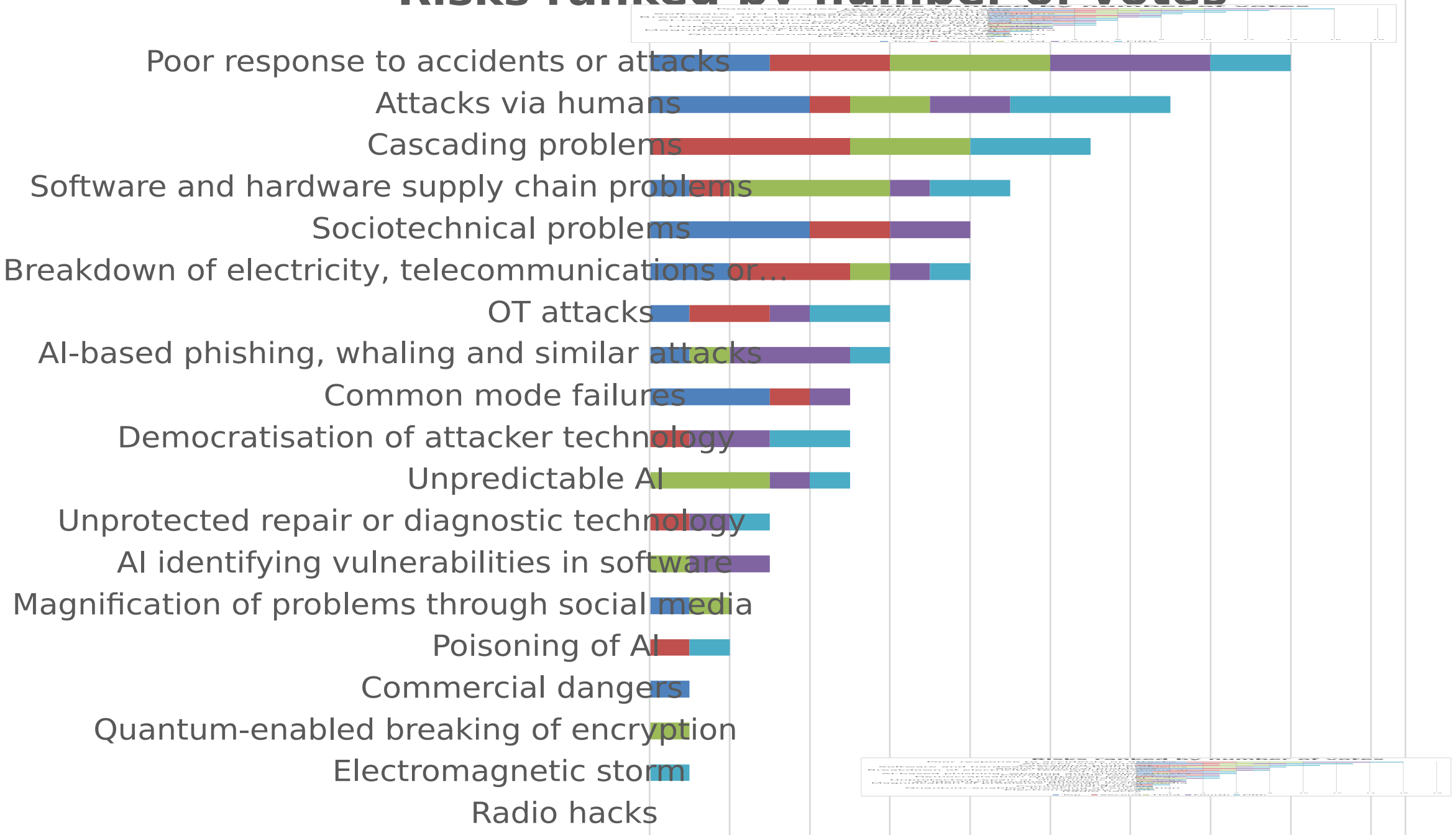


Delphi Study

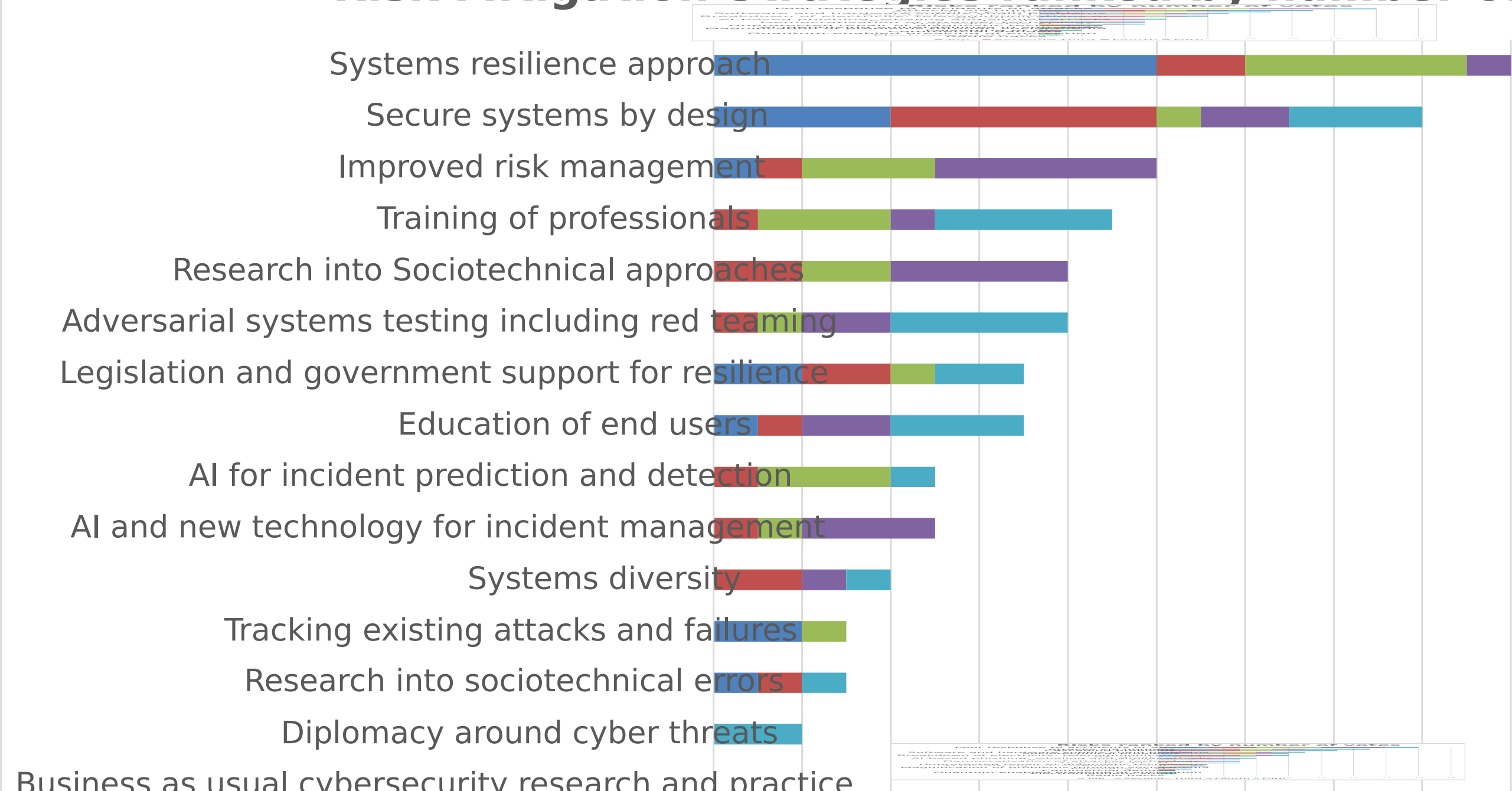
Trends

- Off the shelf hardware and software
- IOT and next generation technologies
- System complexity and interconnectivity
- Increase in digitisation
- Decentralisation of services
- New CNI
- Increase in end-user dependence on technology
- System operators working only through software
- Changing geopolitical context
- Artificial intelligence
- Quantum computing

Risks ranked by number of votes



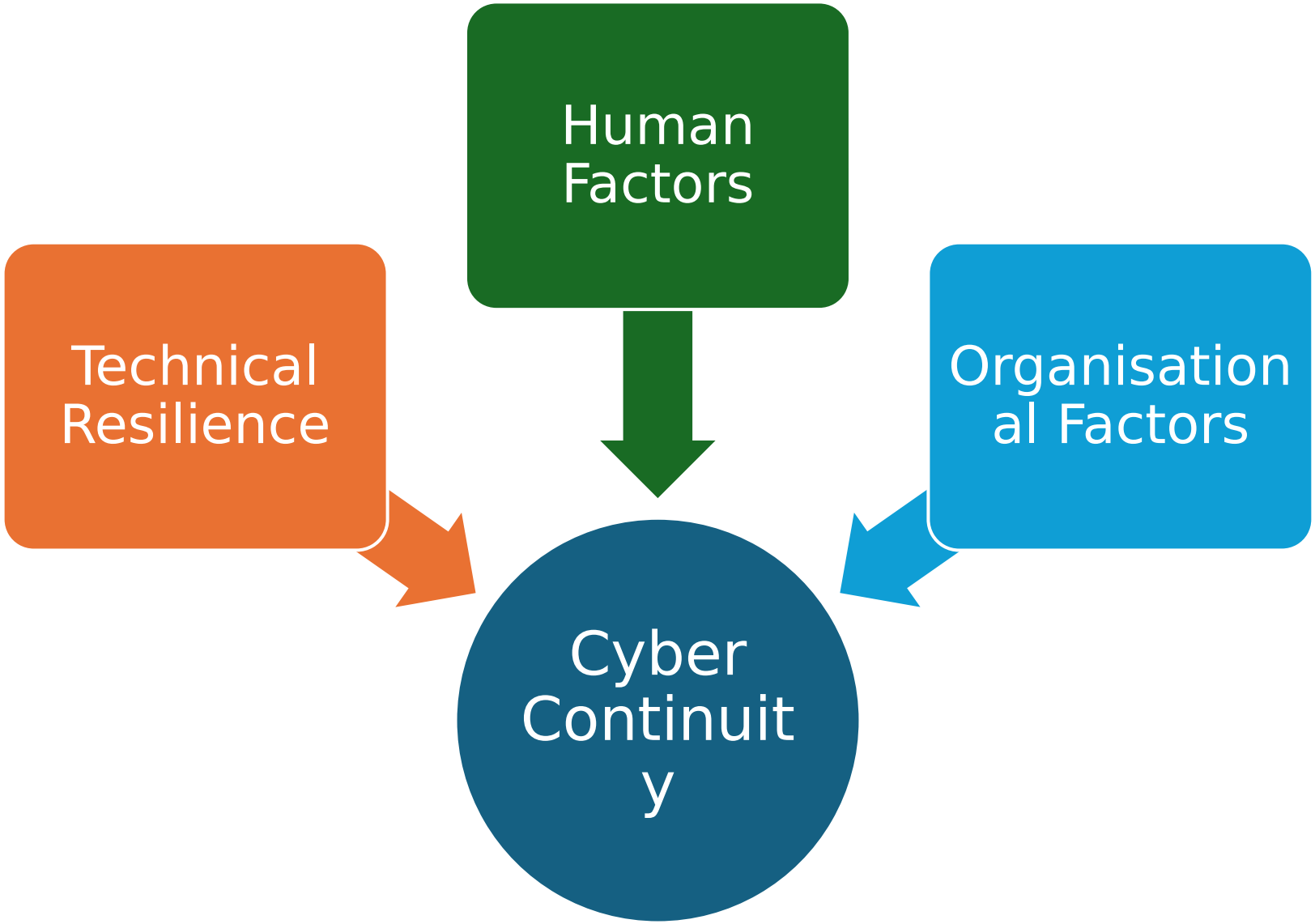
Risk Mitigation Strategies ranked by number of




Systems
Resilience?

Cyber Service Resilience/Cyber Continuity!

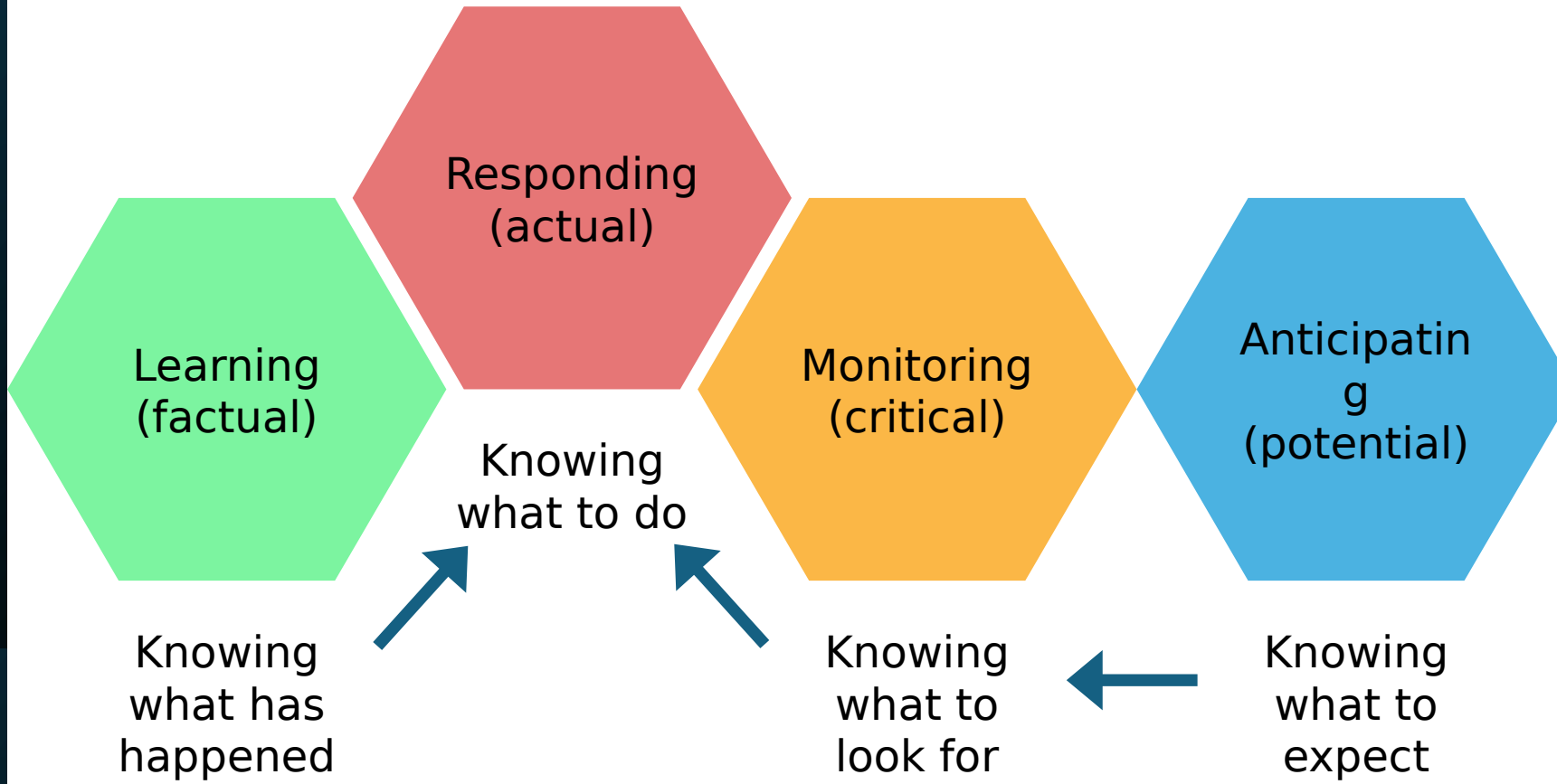
- Scenario:
  - Organisation has major software systems disaster:
  - Many bad outcomes: death and suffering; stress and breakdowns; financial; reputational.
  - Many of the outcomes are outside the organisation.
- What kinds of things reduce (mitigate) these outcomes?
- What are inexpensive prior mitigations?
- And how do we justify (sell) them, now?


Human Factors
Technical Resilience
Organisational Factors
Cyber Continuity

NIST Cybersecurity Framework (CSF) 2.0, Feb. 2024

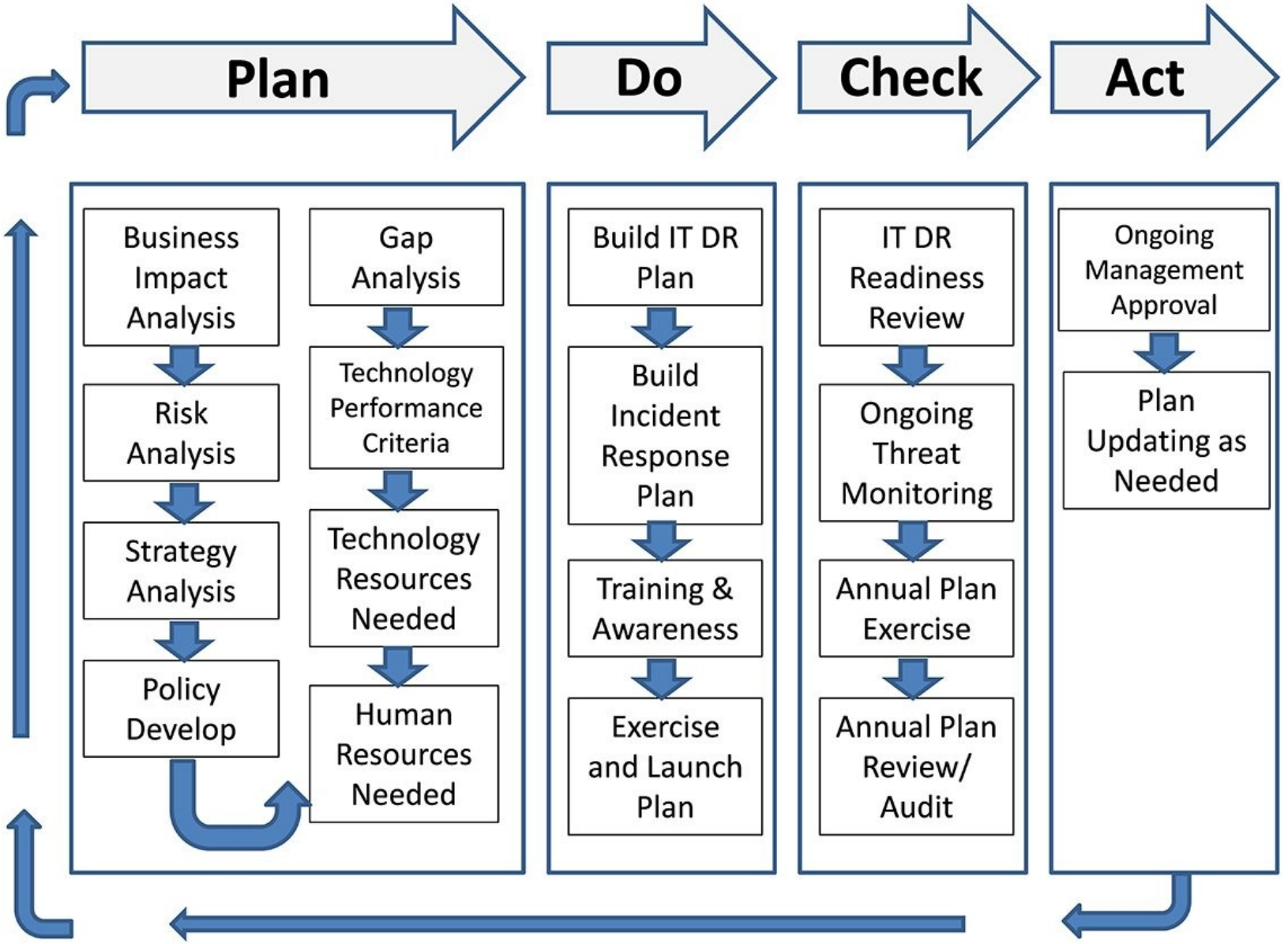
Resilience from a Cyber Perspective

Resilience Engineering Perspective



- *E. Hollnagel, The Four Cornerstones of Resilience Engineering, in Resilience Engineering Perspectives: Preparation and Restoration*

Business Continuity Perspective



Cyber Service Resilience Literature?

- S. M. Alhidaifi, M. R. Asghar, and I. S. Ansari, “A Survey on Cyber Resilience: Key Strategies, Research Challenges, and Future Directions,
- D. S. Fowler, G. Epiphaniou, M. D. Higgins, and C. Maple, “Aspects of Resilience for Smart Manufacturing Systems,”
- T. N. I. Alrumaih, M. J. F. Alenazi, N. A. AlSowaygh, A. A. Humayed, and I. A. Alablani, “Cyber Resilience in Industrial Networks: A State of the Art, Challenges, and Future Directions,”
- A. Annarelli, F. Nonino, and G. Palombi, “Understanding the Management of Cyber Resilient Systems.
- S. S. Bagheri, G. Ridley, and B. Williams, “Organisational Cyber Resilience: Management Perspectives”

Cyber Service Resilience Regulation?

- The EU Cybersecurity Act (from 2021)
- The EU NIS 2 Directive (from 2024)
- The EU Cyber Resilience Act (from 2027)
- UK NIS Regulations 2018
- UK Product Security and Telecommunications Infrastructure Act 2022 - Part 1
- UK Product Security and Telecommunications Infrastructure (Security Requirements for Relevant Connectable Products) Regulations 2023

- UK Cyber Security and Resilience Bill 2026?
- UK Government Cyber Action Plan 2026
- EU Digital Operational Resilience Act (DORA).

Cyber Continuity Engineering…

- The CrowdStrike incident would have been far less damaging if CrowdStrike had adopted the ‘**canary release**’ practice of updating a subset of the live machines before the rest, allowing the operators to detect the problem and cancel the update before major damage occurred.
- **‘Honeytrap’ fake cards** in a database of payment cards raise an alert when used. By telling the card companies involved, the attacked organisation can then reduce the financial and social damage of a mass data theft.
- A hospital unit hit by a ransomware attack can continue operating if the **data for a period of manual operation** is kept separate from the main computer systems in a human accessible form.

And Cyber Continuity Engineering…

- The British Library scored well on backup, continuity and disaster planning. But two years after their disastrous ransomware attack many of their outdated systems still cannot be restored. So, regular **system rebuilds from backup**?
- Often (Colonial Pipeline, Skype), the accounting/auditing systems fail; the service can still run. So, plan for a '**Free Beer Day**', where the service continues.
- M&S and CoOp both had similar cyberattacks; we understand M&S suffered more because the CoOp team shut down their systems more quickly. Plan a '**big red button**' to disable systems and agree when to use it?



Charles Weir
Cecilia Loureiro-Koechlin
Louise Dennis
Lucy Hunt
Ita Ryan

https://lancaster.ac.uk/

North West Partnership
for Security and Trust

GCHQ MANCHESTER 1824 The University of Manchester Lancaster University Manchester Metropolitan University University of Salford MANCHESTER